



# FortiSwitch Release Notes

Version 6.4.3

## **FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

## **FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

## **FORTINET BLOG**

<https://blog.fortinet.com>

## **CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

## **FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

## **FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

## **FORTIGUARD CENTER**

<http://www.fortiguard.com>

## **FORTICAST**

<http://forticast.fortinet.com>

## **END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

## **FORTINET PRIVACY POLICY**

<https://www.fortinet.com/corporate/about-us/privacy.html>

## **FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



FortiSwitch Release Notes

October 29, 2020

11-643-646835-20201029

# TABLE OF CONTENTS

<b>Change log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
Supported models	5
What's new in FortiSwitchOS 6.4.3	5
<b>Special notices</b>	<b>8</b>
Supported features for FortiSwitchOS 6.4.3	8
Connecting multiple FSR-112D-POE switches	16
<b>Upgrade information</b>	<b>17</b>
<b>Product integration and support</b>	<b>18</b>
FortiSwitch 6.4.3 support	18
<b>Resolved issues</b>	<b>19</b>
<b>Known issues</b>	<b>20</b>

## Change log

Date	Change Description
October 29, 2020	Initial release for FortiSwitchOS 6.4.3

# Introduction

This document provides the following information for FortiSwitch 6.4.3 build: 0452.

- [Supported models on page 5](#)
- [Special notices on page 8](#)
- [Upgrade information on page 17](#)
- [Product integration and support on page 18](#)
- [Resolved issues on page 19](#)
- [Known issues on page 20](#)

See the [Fortinet Document Library](#) for FortiSwitch documentation.

## Supported models

FortiSwitch 6.4.3 supports the following models:

<b>FortiSwitch 1xx</b>	FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE
<b>FortiSwitch 2xx</b>	FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE
<b>FortiSwitch 4xx</b>	FS-424D, FS-424D-FPOE, FS-424D-POE, FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448D, FS-448D-FPOE, FS-448D-POE, FS-448E, FS-448E-POE, FS-448E-FPOE
<b>FortiSwitch 5xx</b>	FS-524D-FPOE, FS-524D, FS-548D, FS-548D-FPOE
<b>FortiSwitch 1xxx</b>	FS-1024D, FS-1048D, FS-1048E
<b>FortiSwitch 3xxx</b>	FS-3032D, FS-3032E
<b>FortiSwitch Rugged</b>	FSR-112D-POE, FSR-124D

## What's new in FortiSwitchOS 6.4.3

Release 6.4.3 provides the following new features:

- You can now view the details of bidirectional forwarding detection (BFD) neighbors by going to *Router > Monitor > BFD Neighbor*.
- You can now view the flow-export data by going to *System > Flow Export > Monitor*.

- All log entries can now be viewed from the *Log > Entries* page; they can be filtered by subtype, level, user, user interface, action, and status. A new *Delete All* button allows you to delete all log entries.
- Packet capture is now supported in the GUI, as well as the CLI and REST API.
- You can now view or clear all access control list (ACL) counters by going to *Switch > Monitor > ACL Counters*.
- You can now check the VRRP status by going to *Router > Monitor > VRRP*.
- You can now configure the IGMP-snooping querier version 2 or 3. When the IGMP querier version 2 is configured, the FortiSwitch unit will send IGMP queries version 2 when no external querier is present. When the IGMP querier version 3 is configured, the FortiSwitch unit will send IGMP queries version 3 when no external querier is present.
- More services are available when configuring the classifier in the GUI for the egress and prelookup policies.
- Media Access Control security (MACsec) is now supported.
- You can now use the `diagnose switch physical-ports qos-rates list [<list_of_ports>]` command to view the real-time egress QoS queue rates, including the data rate, line rate, and drop rate.
- When a neighboring router has a graceful restart, the FortiSwitch unit now enters the helper (neighbor) mode and keeps the restarting router in the forwarding path for OSPF routing.
- OSPF database overflow protection is now supported.
- IPv6 support has been expanded. You can now use IPv6 addresses with BGP routing, IS-IS routing, and RIP routing. Multicast Listener Discovery (MLD) snooping, MLD proxy, and MLD querier are now supported for IPv6 multicast traffic.
- IPv4 and IPv6 static routes now support virtual routing and forwarding (VRF).
- You can now view events that violate the IP source-guard settings with the IP source-guard violation log.
- You can now specify system banner messages in the CLI that will appear when users log in using either the CLI or the GUI.
- You can now configure the maximum burst size allowed by storm control per port or per switch.
- You can use the new `diagnose certificate {all | ca | local | remote}` commands to verify your system certificates.

The following REST API changes were made in this release:

- You can now use the current release version in the FortiSwitch REST API requests (`https://<switch_IP_address>/api/v<x.x.x>/`) to get the latest (v6.4.3) schema content in the response. You can still use FortiSwitch REST API requests with `https://<switch_IP_address>/api/v2/` to get the older v2 schema in the response.
- The `monitor/switch/log` endpoint is now `monitor/system/log`.
- The new `cmdb/router/ripng` endpoint supports RIP routing for IPv6 traffic.
- The new `cmdb/switch.mld-snooping/globals` endpoint supports MLD snooping.
- The `cmdb/router/route-map` endpoint now supports RIP routing for IPv6 traffic and IS-IS routing for IPv6 traffic.
- The `cmdb/router/isis` endpoint now supports IS-IS routing for IPv6 traffic.
- The `cmdb/router/bgp` endpoint now supports BGP routing for IPv6 traffic.
- The `cmdb/system/global` endpoint now supports specifying system banner messages that will appear when users log in using either the CLI or the GUI.
- The `cmdb/switch/physical-port` endpoint and the `cmdb/switch/storm-control` endpoint now support configuring the maximum burst size allowed by storm control.

The following CLI changes were made in this release:

- Under the `config router ospf` command, the `set default-information-route-map` command has been removed.

- Under the `config router isis` command, the `set default-information-route-map` command has been removed.
- Under the `config switch vlan` command, `set igmp-fast-leave` is now `set igmp-snooping-fast-leave`.
- Under the `config switch vlan` command, `set igmp-proxy` is now `set igmp-snooping-proxy`.
- Under the `config switch vlan` command, `set querier-addr` is now `set igmp-snooping-querier-addr`.
- Under the `config switch vlan` command, `config igmp-static-group` is now `config igmp-snooping-static-group`.
- Under the `config switch interface` command, `set igmps-flood-reports` is now `set igmp-snooping-flood-reports`.
- Under the `config switch interface` command, `set igmps-flood-traffic` is now `set mcast-snooping-flood-traffic`.
- The `set flood-unknown-multicast` command moved from under `config switch igmp-snooping globals` to under `config switch global`.
- The `get switch igmp-snooping interface` command was replaced with `get switch igmp-snooping status`.
- The `diagnose debug application igmp_snooping` command is now `diagnose debug application mcast-snooping`.
- Under the `config router bgp` command, `set aspath-filter-list-in` is now `set filter-list-in`.
- Under the `config router bgp` command, `set aspath-filter-list-out` is now `set filter-list-out`.
- Under the `config router bgp` command, `log-neighbor-changes` is now `set neighbour-changes`.

## Special notices

### Supported features for FortiSwitchOS 6.4.3

The following table lists the FortiSwitch features in Release 6.4.3 that are supported on each series of FortiSwitch models. All features are available in Release 6.4.3, unless otherwise stated.

Feature	GUI supported	112D-POE	FSR-124D	1xxE 1xxF	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
<b>Management and Configuration</b>									
CPLD software upgrade support for OS	—	—	—	—	—	—	—	1024D 1048D	—
Firmware image rotation (dual-firmware image support)	—	✓	✓	148E 148E-POE	✓	✓	✓	✓	✓
HTTP REST APIs for configuration and monitoring	—	✓	✓	✓	✓	✓	✓	✓	✓
Support for switch SNMP OID	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP conflict detection and notification	✓	✓	✓	✓	✓	✓	✓	✓	✓
FortiSwitch Cloud configuration	✓	✓	✓	✓	✓	✓	✓	✓	✓
Auto topology	—	✓	✓	✓	✓	✓	✓	✓	✓
<b>Security and Visibility</b>									
802.1x port mode	✓	✓	✓	✓	✓	✓	✓	✓	✓
802.1x MAC-based security mode	✓	✓	✓	✓	✓	✓	✓	✓	✓



Feature	GUI supported	112D-POE	FSR-124D	1xxE 1xxF	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
User-based (802.1x) VLAN assignment	✓	✓	✓	✓	✓	✓	✓	✓	✓
802.1x enhancements, including MAB	✓	✓	✓	✓	✓	✓	✓	✓	✓
MAB reauthentication disabled	—	✓	✓	✓	✓	✓	✓	✓	✓
open-auth mode	✓	✓	✓	✓	✓	✓	✓	✓	✓
Support of the RADIUS accounting server	Partial	✓	✓	✓	✓	✓	✓	✓	✓
Support of RADIUS CoA and disconnect messages	—	✓	✓	✓	✓	✓	✓	✓	✓
EAP Pass-Through	✓	✓	✓	✓	✓	✓	✓	✓	✓
Network device detection	—	—	✓	—	✓	✓	✓	✓	✓
IP-MAC binding (IPv4)	✓	—	—	—	—	—	✓	✓	✓
sFlow (IPv4)	✓	✓	✓	—	✓	✓	✓	✓	✓
Flow export (IPv4)	✓	—	✓	—	✓	✓	✓	✓	✓
ACL (IPv4)	✓	—	✓	✓	✓	✓	✓	✓	✓
Multistage ACL (IPv4)	✓	—	—	—	—	—	✓	✓	✓
Multiple ingress ACLs (IPv4)	✓	—	✓	—	✓	✓	✓	✓	✓
Schedule for ACLs (IPv4)	—	—	✓	✓	✓	✓	✓	✓	✓
DHCP snooping	✓	✓	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE 1xxF	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
DHCPv6 snooping	✓	—	—	—	✓	✓	✓	✓	✓
Allowed DHCP server list	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP source guard (IPv4)	✓	—	✓	—	✓	✓	—	—	—
IP source-guard violation log	—	—	✓	—	✓	✓	—	—	—
Dynamic ARP inspection (IPv4)	✓	—	✓	✓	✓	✓	✓	✓	✓
ARP timeout value	—	✓	✓	✓	✓	✓	✓	✓	✓
Access VLANs	—	✓	✓	✓	✓	✓	✓	✓	✓
RMON group 1	—	✓	✓	✓	✓	✓	✓	✓	✓
Reliable syslog	—	✓	✓	✓	✓	✓	✓	✓	✓
Packet capture	✓	—	✓	—	✓	✓	✓	✓	✓
MACsec (See Note 7.)	—	—	—	—	—	—	✓	—	—
<b>Layer 2</b>									
Link aggregation group size (maximum number of ports) (See Note 2.)	✓	8	8	8	8	8	24/48	24/48	24 64
LAG min-max-bundle	—	✓	✓	✓	✓	✓	✓	✓	✓
IPv6 RA guard	—	—	—	—	✓	✓	✓	✓	✓
IGMP snooping	✓	✓	✓	✓	✓	✓	✓	✓	✓
IGMP proxy	✓	✓	✓	✓	✓	✓	✓	✓	✓
IGMP querier	—	✓	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE 1xxF	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
MLD snooping	—	—	—	—	—	—	✓	✓	✓
MLD proxy	—	—	—	—	—	—	✓	✓	✓
MLD querier	—	—	—	—	—	—	✓	✓	✓
LLDP transmit	—	✓	✓	✓	✓	✓	✓	✓	✓
LLDP-MED	—	✓	✓	✓	✓	✓	✓	✓	✓
LLDP-MED: ELIN support	✓	✓	✓	✓	✓	✓	✓	✓	✓
Per-port max for learned MACs	—	—	✓	✓	✓	✓	✓	—	—
MAC learning limit (See Note 4.)	—	—	✓	✓	✓	✓	✓	—	—
Learning limit violation log (See Note 4.)	—	—	✓	✓	✓	✓	✓	—	—
set mac-violation-timer	—	✓	✓	✓	✓	✓	✓	✓	✓
Sticky MAC	✓	✓	✓	✓	✓	✓	✓	✓	✓
Total MAC entries	—	✓	✓	✓	✓	✓	✓	✓	✓
MSTP instances	—	0-15	0-15	0-15	0-15	0-15	0-32	0-32	0-32
STP root guard	—	✓	✓	✓	✓	✓	✓	✓	✓
STP BPDU guard	✓	✓	✓	✓	✓	✓	✓	✓	✓
Rapid PVST interoperation	—	✓	✓	✓	✓	✓	✓	✓	✓
'forced-untagged' or 'force-tagged' setting on switch interfaces	—	✓	✓	✓	✓	✓	✓	✓	✓
Private VLANs	✓	—	✓	—	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE 1xxF	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Multi-stage load balancing	—	—	—	—	—	—	—	✓	✓
Priority-based flow control	—	—	—	—	—	—	✓	✓	✓
Ingress pause metering	—	—	—	—	✓	✓	✓	✓	3032D
Storm control	✓	✓	✓	✓	✓	✓	✓	✓	✓
Per-port storm control	✓	✓	✓	✓	✓	✓	✓	✓	✓
Global burst-size control	—	✓	✓	✓	✓	✓	✓	✓	✓
MAC/IP/protocol-based VLAN assignment	✓	✓	✓	✓	✓	✓	✓	✓	✓
Virtual wire	✓	—	✓	—	✓	✓	✓	✓	✓
Loop guard	✓	✓	✓	✓	✓	✓	✓	✓	✓
Percentage rate control	✓	—	✓	—	✓	✓	✓	✓	✓
VLAN stacking (QinQ)	—	—	✓	—	✓	✓	✓	✓	✓
VLAN mapping	—	—	✓	—	✓	✓	✓	✓	✓
SPAN	✓	✓	✓	✓	✓	✓	✓	✓	✓
RSPAN and ERSPAN (IPv4)	✓	RSPAN	✓	—	✓	✓	✓	✓	✓
Flow control	—	✓	✓	✓	✓	✓	✓	✓	✓
<b>Layer 3</b>									
Link monitor (IPv4)	✓	✓	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE 1xxF	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Static routing (IPv4/IPv6)	✓	—	✓	—	✓	✓	✓	✓	✓
Hardware routing offload (IPv4/IPv6)	✓	—	✓	—	✓	✓	✓	✓	✓
Software routing only (IPv4/IPv6)	✓	✓	—	✓	—	—	—	—	—
OSPF (IPv4/IPv6) (See Note 3.)	✓	—	—	—	✓	✓	✓	✓	✓
OSPF database overflow protection (IPv4)	—	—	—	—	✓	✓	✓	✓	✓
OSPF graceful restart (helper mode only) (IPv4)	—	—	—	—	✓	✓	✓	✓	✓
RIP (IPv4/IPv6) (See Note 3.)	✓	—	—	—	✓	✓	✓	✓	✓
VRRP (IPv4/IPv6) (See Note 3.)	✓	—	—	—	✓	✓	✓	✓	✓
BGP (IPv4/IPv6) (See Note 3.)	—	—	—	—	—	—	✓	✓	✓
IS-IS (IPv4/IPv6) (See Note 3.)	—	—	—	—	✓	✓	✓	✓	✓
PIM (IPv4) (See Note 3.)	—	—	—	—	—	—	✓	✓	✓
Hardware-based ECMP (IPv4)	—	—	—	—	—	—	✓	✓	✓
VRF (IPv4/IPv6)	—	—	—	—	—	—	—	✓	✓
Static BFD (IPv4/IPv6)	✓	✓	✓	✓	✓	✓	✓	✓	✓
BFD for BGPv6	—	—	—	—	—	—	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE 1xxF	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
BFD for RIPvng	—	—	—	—	✓	✓	✓	✓	✓
uRPF	—	—	—	—	—	—	✓	✓	✓
DHCP relay (IPv4)	✓	—	✓	✓	✓	✓	✓	✓	✓
DHCP server (IPv4)	✓	—	—	—	✓	4xx only	✓	✓	✓
<b>High Availability</b>									
MCLAG (multichassis link aggregation)	Partial	—	—	—	✓	✓	✓	✓	✓
STP supported in MLAGs	—	—	—	—	✓	✓	✓	✓	✓
IGMP snooping support in MLAG	✓	—	—	—	✓	✓	✓	✓	✓
<b>Quality of Service</b>									
802.1p support, including priority queuing trunk and WRED	✓	—	✓	✓	✓	✓	✓	✓	✓
QoS queue counters	—	—	✓	—	✓	✓	✓	✓	✓
QoS marking (IPv4/IPv6)	—	—	✓	—	✓	✓	✓	✓	✓
Summary of configured queue mappings	✓	—	✓	✓	✓	✓	✓	✓	✓
Egress priority tagging (IPv4/IPv6)	—	—	✓	—	✓	✓	✓	✓	✓
ECN (IPv4/IPv6)	—	—	—	—	✓	—	✓	✓	✓
Real-time egress queue rates	—	—	—	—	—	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE 1xxF	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
<b>Miscellaneous</b>									
PoE-pre-standard detection (See Note 1.)	—	✓	✓	FS-1xxE POE	✓	✓	✓	—	—
PoE modes support: first come, first served or priority based (PoE models)	—	✓	✓	FS-1xxE POE	✓	✓	✓	—	—
Control of temperature alerts	—	✓	✓	—	✓	✓	✓	✓	✓
Split port (See Note 6.)	Partial	—	—	—	—	—	✓	1048E	✓
TDR (time-domain reflectometer)/cable diagnostics support	✓	—	✓	✓	✓	✓	✓	—	—
Auto module max speed detection and notification	✓	—	—	—	—	—	✓	✓	—
Monitor system temperature (threshold configuration and SNMP trap support)	—	✓	✓	FS-124E-POE FS-124E-FPOE FS-148E FS-148E-POE	✓	✓	✓	✓	✓
Cut-through switching	—	—	—	—	—	—	—	✓	✓
Add CLI to show the details of port statistics	—	✓	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE 1xxF	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Configuration of the QSFP low-power mode	—	—	—	—	—	—	✓	1048D 1048E	✓
Energy-efficient Ethernet	✓	✓	✓	✓	✓	✓	✓	—	—
PHY Forward Error Correction (see Note 5)	—	—	—	—	—	—	—	1048E	3032E
PTP transparent clock (IPv4/IPv6)	—	—	—	—	✓	✓	✓	1048E	✓

### Notes

- PoE features are applicable only to the model numbers with a POE or FPOE suffix.
- 24-port LAG is applicable to 524D, 524-FPOE, 1024D, and 3032D models. 48-port LAG is applicable to 548D, 548-FPOE, and 1048D models.
- To use the dynamic layer-3 protocols, you must have an advanced features license.
- The per-VLAN MAC learning limit and per-trunk MAC learning limit are not supported on the 448D/448D-POE/448D-FPOE/248E-POE/248E-FPOE/248D series.
- Supported only in 100G mode (clause 91).
- On the 3032E, you can split one port at the full base speed, split one port into four sub-ports of 25 Gbps each (100G QSFP only), or split one port into four sub-ports of 10 Gbps each (40G or 100G QSFP).
- Supported on 5xxD 10G ports.

## Connecting multiple FSR-112D-POE switches

The FSR-112D-POE switch does not support interconnectivity to other FSR-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.



# Upgrade information

FortiSwitch 6.4.3 supports upgrading from FortiSwitch 3.5.0 and later.

For FortiSwitch units managed by FortiGate units, refer to the *FortiSwitch Devices Managed by FortiOS Release Notes* for upgrade information. See <https://docs.fortinet.com/document/fortiswitch/6.4.3/managed-switch-release-notes>.

# Product integration and support

## FortiSwitch 6.4.3 support

The following table lists 6.4.3 product integration and support information.

<b>Web browser</b>	<ul style="list-style-type: none"><li>• Mozilla Firefox version 52</li><li>• Google Chrome version 56</li></ul> Other web browsers may function correctly, but are not supported by Fortinet.
<b>FortiOS (FortiLink Support)</b>	FortiLink is supported on all FortiSwitch models when running FortiOS 5.4.0 and later and FortiSwitchOS 3.2.1 and later.

## Resolved issues

The following issues have been fixed in FortiSwitchOS 6.4.3. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
615591	For power supply unit (PSU) sensors on supported hardware, the value of EntitySensorStatus will be 1 (ok) if the sensor has detected that the PSU is inserted/connected. If the PSU is not inserted (or the sensor operational status is unavailable on that platform), the value is 2 (unavailable).
629721	HTTP and HTTPS connections from the same client or from the same browser do not work.
645993	When IGMP snooping is enabled, IGMP packets are being forwarded out of the MRP blocking port, which causes a loop.
646555	The <code>set mirror qos</code> command (under the <code>config switch global</code> command) is available but not functional.
648046, 649564	The network cannot be accessed because of an STP loop in a closed ring topology.
648356	When a new MSTP instance is created on a switch for any particular VLAN, the trunk with the FortiGate unit on the new instance shows a mismatch on the port that is connected to the FortiGate unit.
653907	After FortiSwitch units were replaced, three APC network management cards and a Zebra printer cannot be accessed.
658968	The syslog source IP address is a loopback IP address, but the interface is still sending syslog data.
662110	A Fortinet module is causing a critical-level message, "Non-Fortinet Module Inserted."
663466	You cannot use the zero-touch configuration in FortiSwitch Cloud to change the admin password.

# Known issues

The following known issues have been identified with FortiSwitchOS 6.4.3. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
382518, 417024, 417073, 417099, 438441	DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANS).
414972	IGMP snooping might not work correctly when used with 802.1x Dynamic VLAN functionality.
480605	<p>When DHCP snooping is enabled on the FSR-112D-POE, the switched virtual interface (SVI) cannot get the IP address from the DHCP server.</p> <p><b>Workarounds:</b></p> <ul style="list-style-type: none"><li>—Use a static IP address in the SVI when DHCP snooping is enabled on that VLAN.</li><li>—Temporarily disable dhcp-snooping on vlan, issue the <code>execute interface dhcpclient-renew &lt;interface&gt;</code> command to renew the IP address. After the SVI gets the IP address from the DHCP server, you can enable DHCP snooping.</li></ul>
510943	<p>The time-domain reflectometer (TDR) function (cable diagnostics feature) reports unexpected values.</p> <p><b>Workaround:</b> When using the cable diagnostics feature on a port (with the <code>diagnose switch physical-ports cable-diag &lt;physical port name&gt;</code> CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.</p>
520954	When a “FortiLink mode over a layer-3 network” topology has been configured, the FortiGate GUI does not always display the complete network.
542031	For the 5xx switches, the <code>diagnose switch physical-ports led-flash</code> command flashes only the SFP port LEDs, instead of all the port LEDs.
548783	Some models support setting the mirror destination to “internal.” This is intended only for debugging purposes and might prevent critical protocols from operating on ports being used as mirror sources.

Bug ID	Description
572052	<p>Backup files from FortiSwitchOS 3.x that have 16-character-long passwords fail when restored on FortiSwitchOS 6.x. In FortiSwitchOS 6.x, file backups fail with passwords longer than 15 characters.</p> <p><b>Workaround:</b> Use passwords with a maximum of 15 characters for FortiSwitchOS 3.x and 6.x.</p>
585550	<p>When packet sampling is enabled on an interface, packets that should be dropped by uRPF will be forwarded.</p>
606044	<p>The value for cable length is wrong when running cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.</p>
609375	<p>The FortiSwitchOS supports four priority levels (critical, high, medium, and low); however, The SNMP PowerEthernet MIB only supports three levels. To support the MIB, a power priority of medium is returned as low for the PoE MIB.</p>
610149	<p>The results are inaccurate for open and short cables when running cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.</p>
617755	<p>The internal interface cannot obtain IPv6 addresses with dhcpv6-snooping enabled on the native VLAN.</p>



**FORTINET®**



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.